that upon tampering with the secure housing the second memory is disconnected from the battery, said postal security device further comprising an encryption key stored within said second memory, said postal security device further comprising a cryptographic engine; the method comprising the steps of:

storing the encryption key within the second memory;

encrypting the body of data by the cryptographic engine with respect to the encryption key;

storing the encrypted body of data in the first memory;

upon power-up of the postal security device decrypting the encrypted body of data with the cryptographic engine with respect to the encryption key;

temporarily storing the decrypted body of data in a third memory, wherein upon power down of the postal security device the decrypted body of data is lost; and

in the event of tampering with the postal security device, removing power from the second memory and the third memory resulting in a loss of the encryption key and the decrypted body of data.

Please add the following claim(s):

4. (New) A postal security device comprising:

A3

a secure housing, and within the secure housing:

a first nonvolatile memory device not having a backup battery power source and adapted to store an encrypted body of data when power is applied to the postal security device and when power is not applied to the postal security device;

a second nonvolatile memory device having a backup battery power source and having a storage capacity only large enough to store an encryption key;

an encryption engine adapted to encrypt a body of data with reference to the encryption key in order to form the encrypted data stored in the first nonvolatile memory;

A3 Cont'd

a third memory device not having a backup battery and adapted to temporarily store a body of decrypted data while the postal security device is powered on, the body of decrypted data being transferred to the third memory device from the encryption engine when the postal security device is initially powered on, the encryption engine decrypting the decrypted data stored in the second memory device with respect to the encryption key when the postal security device is powered on; and

wherein when the postal security device powers down, the body of decrypted data temporarily stored in the third memory device is lost and battery power required to maintain the postal security device is minimized.

5. (New) The postal security device of claim 4 further comprising a means for generating print data for the printing of

postal indicia, the generating of the print data relying in part on the decrypted body of data.

6. (New) The postal security device of claim 4 further comprising a anti-tamper device adapted to interrupt power to the second memory device and the third memory device when the secure housing of the postal security device is tampered with, wherein the body of decrypted data is lost and the encryption key is not available.

7. (New) The postal security device of claim 4 wherein the body of data includes cryptographic keys and sensitive bit-images.

A3 Contd

8. (New) The postal security device of claim 4 further comprising a detection device adapted to detect that the second non-volatile memory device is no longer storing the encryption key and send a message via a communications channel to a administrator of the postal security device for action.

9. (New) A postal security device having improved battery power consumption during power-off periods comprising:

a first memory device for storing encrypted data, the first memory device being connected to a main power source and not connected to a back-up battery power source;

a second memory device having a memory storage capacity sufficient to store only an encryption key, the encryption

key being used to decrypt the encrypted data stored in the first memory device when the postal security device is powered on, the second memory being connected to both the main power source and the back-up battery power source;

an encryption engine adapted to decrypt the encrypted data using the encryption key during power on; and

a third memory for temporarily storing the decrypted data, the third memory being connected only to the main power source;

wherein when the main power source is interrupted, the decrypted data in the third memory is lost while the second memory retains the encryption key, and since only the second memory requires back-up battery power, battery power consumption of the postal security device is reduced.

A3 contd

10. (New) The postal security device of claim 9 further comprising a anti-tamper device adapted to interrupt power to the second memory device and the third memory device, wherein the body of decrypted data is lost and the encryption key is not available.

11. (New) The postal security device of claim 9 further comprising a postal indicia generator adapted to receive the decrypted body of data from the postal security device over a communications channel and print a postal indicia relying in part of the decrypted body of data.

12. (New) A method of improving back-up battery power consumption in a postal security device comprising:

storing a body of encrypted data in a first memory device that does not have a back-up battery power source, the encrypted data being encrypted by an encryption engine with respect to an encryption key;

storing the encryption key in a second memory device in the postal security device, the second memory device having a back-up battery power source and having a maximum storage capacity limited to a size of the encryption key;

powering up the postal security device and automatically decrypting the encrypted data with respect to the encryption key stored in the second memory device;

A3 Cont'd

temporarily storing the decrypted data in a third memory device not having a back-up power source, wherein if power to the postal security device is interrupted, the decrypted data is lost and only the encryption key stored in the second memory device having the battery back-up is maintained; and

causing the decrypted data in the third memory device and the encryption key to be lost if the postal security device is tampered with.

13. (New) The method of claim 12 further comprising generating an electrical signal when the postal security device is tampered

with that causes the second memory device and the third memory device to automatically clear their respective memories

14. (New) The method of claim 12 further comprising, if the postal security device is tampered with, interrupting main electrical power to the second memory and the third memory and interrupting back-up electrical power to the second memory, wherein the interruption of main and back-up electrical power causes the second memory and the third memory to be cleared.

15. (New) The method of claim 12 further comprising minimizing an amount of back-up battery power consumed by the postal security device when the postal security device is powered down by requiring back-up power only for the second memory.

A3 Contd

16. (New) The method of claim 12 further comprising storing only the encryption key and the encrypted body of data when no power is supplied to the postal security device and only the back-up power is supplied to the second memory device.

17. (New) The method of claim 12 further comprising generating a postal indicia relying in part on the decrypted body of data and transmitting the postal indicia over a communications channel to a printer for printing the postal indicia.

18. (New) The method of claim 2 further comprising, upon power-up of the postal security device, detecting a presence of the encryption key, and if not present, transmitting a message

to an administrator of the postal security device indicating a breach of the postal security device.

19. (New) The method of claim 2 further comprising maximizing a life of the battery powering the second memory by limiting a size of data stored in the second memory to the encryption key.

A3 Cont'd.

20. (New) The method of claim 2 further comprising minimizing a need for back-up battery power in the postal security device by only requiring battery power for the second memory, the second memory being limited in data storage capacity size in order to minimize battery power consumption when the second memory relies on back-up battery power.

REMARKS

1. Claim 2 is amended. Claims 1 and 3 are cancelled. Claims 4-20 are new. The specification is amended. Marked up copies of the amended claim and rewritten paragraph are attached hereto.

2. Claim 2 has been amended to overcome the rejection under 35 U.S.C. §112, second paragraph. The change to the specification should also address the Examiner's objection to the drawing. It is only in the specification that the reference character "22" refers to both the bus and the ROM. In the drawing, FIG. 1, the reference characters "22" and "23" are used to designate the ROM and the bus, respectively. These changes do not further limit or narrow the scope of the claim and are not made for reasons related to patentability.